サイバー犯罪（匿名・流動型犯罪）対応

米国におけるサイバー犯罪

全米での被害実態
●2024年のインターネット関連犯罪被害額は166億ドル。１日平均の被害申告は2,000件を超えた。申告１件あたりの被害額は19,372ドル。

テネシー州の被害実態（主な手口と件数：2024年）
●架空請求詐欺　135件
●ビジネスメール　377件
●政府機関員なりすまし　468件
●ロマンス詐欺　411件
●クレジットカード詐欺　307件
●恐喝　1,729件
●フィッシング詐欺　1,026件
●投資詐欺　626件
●技術サポート詐欺　672件
●未払い/未配達　960件

※テネシー州捜査局提供

米国における詐欺事件

〇当館で把握している詐欺事件の主な手口（ニセ警察詐欺１）

１　銀行・クレジットカード会社を騙る者から着信。
「不審な支払いがあるが問題ないか？」「偽造カードを作られているようだ」
「FBIに転送するから、被害申告をしてほしい」
２　偽FBI捜査官に転送
基本的には親身になって、話を聞いてくれる。
しかし「偽造カードの存在により、あなたの名前が大きな犯罪組織の構成員として捜査線上に挙がっている」「数日以内にあなたの事件が起訴される」「今のところ無実を立証するものはなく、起訴されれば拘束される」「公判は時間がかかるため拘束は長期間になる」などと不安を煽る。
偽FBIは無実証明のため、親身になって対策を考える。
３　偽判事なども登場し、信憑性を深めていく。
４　資金窃取の動き
「捜査のため」を口実に「保有財産を指定する口座に移動させる」「ドルを仮想通貨に変えさせる」「金を購入させ、指定住所に送付させる」
５　パスワードなどの窃取
上記やり取りの中で、関係性を構築し、巧みに資金を保管している口座やアプリ等のID・パスワード等を聞き取る。

米国における詐欺事件

〇当館で把握している詐欺事件の主な手口（ニセ警察詐欺2）

1　在米総領事館員を名乗る者から着信。
　各地の実在する総領事館員を名乗り「犯罪に巻き込まれている」「犯罪グループの一員として名前が挙がっている」などと日本語で不安を煽る。

2　偽警視庁捜査員に転送
　親身になって、話を聞いてくれるが「あなたが、大きな犯罪組織の構成員として捜査線上に挙がっている」などと不安を煽る。

直近半年で、在アメリカ合衆国日本国大使館、ヒューストン、アトランタ、ロサンゼルス、シカゴ、ニューヨーク各総領事館員を名乗るケースが確認されている。

米国における詐欺事件

○当館で把握している詐欺事件の主な手口（その他）

１　税関職員を騙るケース
　「荷物に禁制品が入っている」→捜査当局に繋がる（日本語・英語）→様々な理由を付けて、金銭の支払いを迫る。

２　当地裁判所を騙るケース
　「陪審員に選定されていたにも関わらず、これに応じなかった。すぐに罰金を支払う必要がある」

３　技術サポート等
　「これまで無料であったアプリが有料になった」「登録すべき項目が登録されていない。このままだと罰金対象となるが、今なら格安で登録（支援）ができる」

４　ロマンス詐欺
　AIを用いた手口も多い。

５　フィッシング、なりすましメール、投資名目詐欺

詐欺事件への対処

（1）相談する

犯罪組織は「電話を繋げたままにする」「一度電話を切ったとしても、定期的な連絡（行動チェック）を課す」「早期（今すぐ）に行動することを求める」「誰かと相談することを禁止する」等、被害者の動きや思考をコントロールしようとする傾向。

→ 家族を含めた第三者の冷静な判断が有効な対策

「金銭や仮想通貨での支払い」「金や銀の購入（指定場所への郵送）」や「銀行口座や仮想通貨アプリのパスワードの共有」等の話が出た場合は、必ず誰かに相談する。

詐欺事件への対処

（2）冷静な対応と自ら調べる癖をつける

着信画面に表示される電話番号が偽装されることも常套手段の一つ。

相手が当局機関員や日本政府職員等を名乗っていても、安易に信用せず、また、相手が指定する電話番号や住所、転送先も簡単に信用しないようにする。

→「この電話自体の真偽を確かめるため、自分から電話をかけ直したい。所属機関と住所・電話番号を教えてほしい」と提案

→自身で「当該機関が実在するのか」「電話番号や住所は間違いないか」をインターネット等により確認した上、当該機関の電話番号に連絡し、担当者を呼び出す。

詐欺事件への対処

（３）当館への連絡

特殊詐欺が疑われる事件に遭遇した際には、当館までご連絡をお願いします。

日本の大使館・総領事館が逮捕や強制送還を示唆したり、金銭・仮想通貨等を求めたりすることはありません。